

Karamveer Singh Sidhu

Deep Learning Researcher | Full-Stack Software Engineer

karamveersidhu14@gmail.com | Prince George, BC, Canada | karamveersidhu.com | LinkedIn | GitHub

Skills

Languages: Python, TypeScript, JavaScript, C++, SQL

Frontend/Backend: React.js, Next.js, Node.js, NestJS, REST APIs, BullMQ, OAuth, Web3, Design Systems

ML/Data/Infra: PyTorch, Flower, Federated Learning, PostgreSQL, MongoDB, Redis, Docker, AWS

Experience

Tokenbooks

June 2025 – Present

Software Engineer

Vancouver, BC

- Built AI-agent skills/harnesses for guided workflows, deterministic checks, and safer monorepo navigation.
- Built Web3 finance workflows across wallet/exchange sync, accounting, reporting, payments, approvals, and payouts.
- Improved ingestion reliability with async jobs, status tracking, structured errors, OAuth reconnects, and XLSX exports.

University of Northern British Columbia

Sept. 2024 – June 2025

Graduate Teaching Assistant

Prince George, BC

- Designed and delivered labs for 110+ students covering statistics and visualization with R and R Commander.
- Developed Jupyter/Python labs, taught statistical modeling concepts, provided student support, and assisted with grading and exam invigilation.

CloudSEK

July 2022 – Aug. 2024

Software Development Engineer

Bangalore, India

- Built data visualization components, dashboards, and user-facing pages for flagship products XVigil and SVigil. Contributed to in-house design system components.
- Implemented chunked APK uploads, reducing upload time by 40–50% while bypassing file size limits.
- Developed Exposure Search with other engineers, contributing to 100k+ searches and 3000+ leads; independently shipped a new product frontend within two weeks, supporting a \$100k deal.

Research

MSc Thesis Research: Causal FL-IDS Defense

Sept. 2024 – June 2026

Causal Structure Learning for Adversarial Robustness in Federated Learning | GitHub

- Implemented causal structure learning for adversarial robustness in Federated Learning, CNN based Intrusion Detection Systems.
- Used a learnable sparse 64x64 causal matrix, aggregated across clients with FedAvg.
- Built a UM-NIDS pipeline to merge multiple datasets and evaluated a 4-client non-IID PyTorch, Flower setup under FGSM and PGD attacks.
- Improved PGD robustness from 41.0% to 89.85% at $\epsilon = 0.20$ with under 1% clean-accuracy loss, without adversarial training.
- Co-authored an SoK with University of Louisiana at Lafayette researchers on healthcare LLM privacy threats, defenses, and recommendations.

Mitacs Globalink Research Award: Research Internship

Jan. 2026 – Mar. 2026

City, University of London | 12-week research internship

- Awarded the Mitacs Globalink Research Award to conduct a 12-week research internship at City, University of London.
- Researched and implemented the core causal structure learning algorithm for improving the adversarial robustness of a CNN-based Intrusion Detection System.

Education

University of Northern British Columbia

Sept. 2024 – June 2026

MSc, Computer Science

GPA: 4.08

Thesis: Causal Structure Learning for Adversarial Robustness in Federated Learning

CNN-based Intrusion Detection Systems are highly vulnerable to adversarial evasion attacks. My research involved using Causal Structure Learning in federated settings to make a CNN model extremely robust to such attacks.

Baba Banda Singh Bahadur Engineering College

2018 – 2022

Bachelor's, Computer Science

CGPA: 8.86

Publications

- **SoK: Privacy-aware LLM in Healthcare: Threat Model, Privacy Techniques, Challenges and Recommendations.** arXiv preprint, 2026.
- **Data science and analytics in agricultural development.** Environment Conservation Journal, 2021.
- **Advancements in farming and related activities with the help of artificial intelligence: a review.** Environment Conservation Journal, 2021.